CYCLIC DIVISION ALGEBRAS AND MAXIMAL TORI

YAO-RUI YEO

Abstract. We show the cardinality of a particular nonabelian cohomology associated to cyclic division algebras is equal to a certain partition number. This computation helps us interpret the number of conjugacy classes of maximal tori defined over an abelian extension.

1. Introduction

The history of cyclic algebras goes back to the 1920s, when Wedderburn proved what is now called Wedderburn's criterion for cyclic division algebras [9]. In particular, Hasse summarized the number theory of cyclic algebras [3] up till what was known then in the 1930s. There has also been the study of cyclic algebras recently. For example, in [4] Hazrat and Wadsworth studied maximal subgroups of the multiplicative group of the quaternions, which is an example of a cyclic division algebra. In [1] Akbari, Ebrahimian, Kermani, and Golsefidy studied maximal subgroups of the general linear group over a division ring, which is related to cyclic algebras as the Artin-Wedderburn theorem implies central simple algebras are isomorphic to a matrix ring over a division ring. Our work in this paper is closely related to understanding maximal tori of cyclic division algebras, which we recall its definition now.

Let K/L be a finite Galois extension, with $\mathrm{Gal}(K/L)$ a cyclic group of order n. Picking $b \in L^\times$ and a generator σ of $\mathrm{Gal}(K/L)$, define the cyclic algebra

$$A := K\{1, j, \dots, j^{n-1}\} \Big/ \begin{array}{c} j^n = b \\ jk = k^\sigma j \text{ for all } k \in K \end{array}.$$

A is a central simple algebra over L, and $[A : L] = n^2$. Our aim is to study the number of maximal tori of the unit group $A^\times$ in the case when A is a cyclic division algebra. In particular, we would like to find a bound for the number of its conjugacy class using cohomological methods.

Note that we can view $A^\times$ as a subgroup of the general linear group $\mathrm{GL}_n(K)$ by looking at the right multiplication map on A. In fact, A is a finite-dimensional simple algebra of rank n^2 over L, and furthermore K is its splitting field, so we have an isomorphism between $A \otimes_L K$ and the set of $n \times n$ matrices over K. This means that $A^\times$ can be viewed as an L-form of $\mathrm{GL}_n(K)$. By using this fact, we can define an action of $\mu_n = \langle\sigma\rangle$ on $\mathrm{GL}_n(K)$ fixing $A^\times$ so that we can make sense of some first nonabelian cohomology groups.

Recall that for a group G and a G-module M, where M is not necessarily abelian, the first nonabelian cohomology is defined to be the set

$$H^1(G, M) := Z^1(G, M) \Big/ \begin{array}{c} \alpha \sim \alpha' \text{ if there exists } \omega \in M \text{ with} \\ \alpha'(g) = \omega\alpha(g)(g \cdot \omega^{-1}) \text{ for all } g \in G \end{array},$$

where $Z^1(G, M)$ is the set of functions $\alpha : G \longrightarrow M$ such that $\alpha(gh) = \alpha(g)(g \cdot \alpha(h))$ for all $g, h \in G$. If M is abelian, $H^1(G, M)$ is simply the first cohomology group $\mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Consider the subgroup $K^\times$ in $A^\times$, and write N to be the normalizer of $K^\times$ in $A^\times$.

Theorem 1.1. *Assume A is a cyclic division algebra. Then $H^1(\mu_n, N)$ injects into the set of n-torsion elements of the symmetric group S_n modulo conjugation. In particular, $H^1(\mu_n, N)$ has cardinality at most p_n, where p_n is the number of partitions $(\lambda_1, \lambda_2, \dots)$ of n such that each λ_i divides n.*

It should be noted that there is a known asymptotic bound for p_n [2]. If we write $\tau(n)$ as the number of divisors of n, then

$$\exp\left(\left(\frac{\tau(n)}{2} - 1\right)\left(\log n + O\left(\frac{\log n}{\log\log n}\right)\right)\right) \leq p_n \leq \exp\left(\frac{\tau(n)\log n}{2} + O(\log\log n)\right).$$

Let us now explain our motivation for, and an interpretation of, theorem 1.1. For any linear algebraic group $\mathbb{G}$ over a field L of characteristic zero, say that a torus T of rank d is a subgroup such that, when viewed over a separable closure L^{sep}, $T(L^{sep})$ is isomorphic to $((L^{sep})^\times)^d$ for some positive integer d, and say T is maximal if $T(L^{sep})$ is maximal in $\mathbb{G}(L^{sep})$. Choose a maximal torus T in $\mathbb{G}$. Over L^{sep}, every maximal torus T is conjugate to one another, implying its rank is well-defined. This is not true if we do not base change up to L^{sep}, so it is of interest to understand the degree in which maximal tori are not conjugate to one another. An approach is via Galois cohomology as outlined below.

If N is the normalizer of a maximal torus T in $\mathbb{G}$, then the quotient $\mathbb{G}/N$ is the set of maximal tori in $\mathbb{G}$. Furthermore, if we let the absolute Galois group $\Gamma = \mathrm{Gal}(L^{sep}/L)$ act on $\mathbb{G}$, then $X = (\mathbb{G}/N)^\Gamma$ is in bijection with the set of maximal L-tori of $\mathbb{G}$ over L. Letting $\mathbb{G}$ act on X by conjugation, the set of $\mathbb{G}^\Gamma$ orbits $\mathrm{Orb}_{\mathbb{G}^\Gamma}(X)$ are the conjugacy classes of maximal L-tori in $\mathbb{G}$. A result of Galois cohomology (see [7] and [8]) tells us that there is a bijection

$$\mathrm{Orb}_{\mathbb{G}^\Gamma}(X) \cong \ker\left(H^1(\Gamma, N) \longrightarrow H^1(\Gamma, \mathbb{G})\right).$$

By letting $\mathbb{G}$ be the general linear group, the nonabelian version of Hilbert's theorem 90 (see [7, chapter III]) tells us that $\mathrm{Orb}_{\mathbb{G}^\Gamma}(X) \cong H^1(\Gamma, N)$. We wish to study the case when $\mathbb{G}^\Gamma = A^\times$. This proves to be a formidable task, so we simplify this problem in this paper by restricting ourselves to looking the the case when we replace Γ by a cyclic group. The fundamental theorem of Galois theory tells us that

$$H^1(\Gamma, N) \cong \varinjlim H^1\left(\mathrm{Gal}\left((L^{sep})^H/L\right), N^H\right)$$

for every open normal subgroup H of Γ such that $(L^{sep})^H/L$ has finite degree. Furthermore, nonabelian cohomology tells us that each set $H^1\left(\mathrm{Gal}\left((L^{sep})^H/L\right), N^H\right)$ injects into $H^1(\Gamma, N)$. Notice that this set computes the conjugacy classes of maximal L-tori in $\mathbb{G}$ that are defined over $(L^{sep})^H$. Therefore our simplification in this paper sheds some light on the original problem. In particular, our computation bounds the number of tori which base changes to the standard maximal one in $\mathrm{GL}_n((L^{set})^H)$ when $(L^{set})^H/L$ is cyclic.

Restricting to the case when Γ is finite, theorem 1.1 implies that there are at most two conjugacy classes for the maximal tori of $A^\times$. This follows from the Artin-Schreier theorem on Γ after noting $p_1 = 1$ and $p_2 = 2$. The case $|\Gamma| = 1$, i.e. that K is separable, is a well-known fact. When $|\Gamma| = 2$, we can further determine that $H^1(\Gamma, N)$ must have cardinality two by demonstrating two functions of $Z^1(G, N)$ that cannot be identified under the equivalence relation (c.f. corollary 2.3).

Theorem 1.1 also tells us an obstruction to proving a result of compact Lie groups to linear algebraic groups. Let G be a compact Lie group with a maximal torus T, and let W be the Weyl group of G with respect to T. Consider its representation ring $R(G)$ over some field k. Then there is a restriction map $R(G) \longrightarrow R(T)^W$, where W acts by conjugation, since representations are isomorphic up to conjugation. A theorem of Cartan-Weyl tells us this restriction map is in fact a ring isomorphism, and the proof of it implicitly uses the fact that maximal tori of compact Lie groups are unique up to conjugation. However, by the discussion above, this is not true in general even for $\mathrm{GL}_n(\mathbb{R})$.

We end the introduction by explaining the organization of the paper. Section 2 explains how we can view $A^\times$ as a subgroup of the general linear group $\mathrm{GL}_n(K)$, so that we can define an action of $\mu_n = \langle\sigma\rangle$ on $GL_n(K)$ fixing $A^\times$ and to make sense of the cohomology group in theorem 1.1. Section 3 proceeds to prove this main theorem using cohomology twisting and the long exact sequence for nonabelian cohomology. After demonstrating why we can always choose $b \in L^\times$ to make cyclic algebras division algebras in section 4, we conclude the paper by giving such choices of b for the algebra $\mathbb{Q}_l[\mu_{p^k}]$.

2. The action of μ_n on $GL_n(K)$

Always let A be a cyclic division algebra unless otherwise stated. Note that we can view $A^\times$ as the following subset

$$\left\{ \begin{bmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ ba_n^\sigma & a_1^\sigma & a_2^\sigma & \cdots & a_{n-2}^\sigma & a_{n-1}^\sigma \\ ba_{n-1}^{\sigma^2} & ba_n^{\sigma^2} & a_1^{\sigma^2} & \cdots & a_{n-3}^{\sigma^2} & a_{n-2}^{\sigma^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ ba_2^{\sigma^{n-1}} & ba_3^{\sigma^{n-1}} & ba_4^{\sigma^{n-1}} & \cdots & ba_n^{\sigma^{n-1}} & a_1^{\sigma^{n-1}} \end{bmatrix} : \text{ not all } a_1, \ldots, a_n \in K \text{ equal zero} \right\}$$

of $GL_n(K)$. This is clear by looking at the matrices gotten from the right multiplication map on A, and in fact a computation tells us this set is in fact a group under matrix multiplication. Hence we can view elements of $A^\times$ as matrices.

We next define the action of μ_n on $GL_n(K)$ that makes sense of the cohomology group in theorem 1.1. Let us recall the following standard result of matrix groups.

Proposition 2.1. *Let N be the normalizer of the standard maximal torus $(K^\times)^n$ in $\mathrm{GL}_n(K)$ respectively, and let $W = N/(K^\times)^n$ be the Weyl group. Then $W \cong S_n$.*

Proof. It is easy to see that the group N consists of the generalized permutation matrices respectively. Therefore its Weyl group has every equivalence class represented by a matrix with value 1 for a nonzero entry and 0 otherwise. □

The next proposition gives us the action we want.

Proposition 2.2. *The action of $\mu_n = \langle\sigma\rangle$ on $GL_n(K)$ fixing $A^\times$ is given by*

$$\sigma \cdot \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \begin{bmatrix} a_{nn}^\sigma & b^{-1}a_{n,1}^\sigma & b^{-1}a_{n,2}^\sigma & \cdots & b^{-1}a_{n,n-2}^\sigma & b^{-1}a_{n,n-1}^\sigma \\ ba_{1,n}^\sigma & a_{1,1}^\sigma & a_{1,2}^\sigma & \cdots & a_{1,n-2}^\sigma & a_{1,n-1}^\sigma \\ ba_{2,n}^\sigma & a_{2,1}^\sigma & a_{2,2}^\sigma & \cdots & a_{2,n-2}^\sigma & a_{2,n-1}^\sigma \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ ba_{n-1,n}^\sigma & a_{n-1,1}^\sigma & a_{n-1,2}^\sigma & \cdots & a_{n-1,n-2}^\sigma & a_{n-1,n-1}^\sigma \end{bmatrix}.$$

The induced action on W is well-defined. Furthermore, $\sigma \cdot \omega = \sigma\omega\sigma^{-1}$ for $\omega \in W$, where we treat σ as the n-cycle $(1\ 2\ \cdots\ n)$ on the right hand side.

Proof. Firstly, to check the given action is a group action we just need to check $\sigma^n(a_{i,j}) = (a_{i,j})$ for any $n \times n$ matrix $(a_{i,j})$ in $GL_n(K)$, since associativity is automatic. This is easy to see by looking at each diagonal, since at some point an $a_{i,j}$ will gain a factor of b and b^{-1} respectively (so they cancel out), and $a_{i,j}^{\sigma^n} = a_{i,j}$. We now need to check this action acts via homomorphisms. By induction it suffices to check this when σ acts on two $n \times n$ matrices (a_{ij}) and (b_{ij}) in $GL_n(K)$. Computing,

$$\begin{aligned} \sigma \cdot ((a_{ij})(b_{ij})) &= \sigma \cdot \begin{bmatrix} \sum_i a_{1,i}b_{i,1} & \cdots & \sum_i a_{1,i}b_{i,n} \\ \vdots & \ddots & \vdots \\ \sum_i a_{n,i}b_{i,1} & \cdots & \sum_i a_{n,i}b_{i,n} \end{bmatrix} \\ &= \begin{bmatrix} \sum_i a_{n,i}^\sigma b_{i,n}^\sigma & b^{-1}\sum_i a_{n,i}^\sigma b_{i,1}^\sigma & \cdots & b^{-1}\sum_i a_{n,i}^\sigma b_{i,n-1}^\sigma \\ b\sum_i a_{1,i}^\sigma b_{i,n}^\sigma & \sum_i a_{1,i}^\sigma b_{i,1}^\sigma & \cdots & \sum_i a_{1,i}^\sigma b_{i,n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots \\ b\sum_i a_{n-1,i}^\sigma b_{i,n}^\sigma & \sum_i a_{n-1,i}^\sigma b_{i,1}^\sigma & \cdots & \sum_i a_{n-1,i}^\sigma b_{i,n-1}^\sigma \end{bmatrix}. \end{aligned}$$

Also we have that

$$\begin{aligned} (\sigma \cdot (a_{ij}))(\sigma \cdot (b_{ij})) &= \begin{bmatrix} a_{nn}^\sigma & b^{-1}a_{n,1}^\sigma & \cdots & b^{-1}a_{n,n-1}^\sigma \\ ba_{1,n}^\sigma & a_{1,1}^\sigma & \cdots & a_{1,n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots \\ ba_{n-1,n}^\sigma & a_{n-1,1}^\sigma & \cdots & a_{n-1,n-1}^\sigma \end{bmatrix} \begin{bmatrix} b_{n,n}^\sigma & b^{-1}b_{n,1}^\sigma & \cdots & b^{-1}b_{n,n-1}^\sigma \\ bb_{1,n}^\sigma & b_{1,1}^\sigma & \cdots & b_{1,n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots \\ bb_{n-1,n}^\sigma & b_{n-1,1}^\sigma & \cdots & b_{n-1,n-1}^\sigma \end{bmatrix} \\ &= \begin{bmatrix} a_{nn}^\sigma b_{nn}^\sigma + \sum_{i<n} b^{-1}a_{n,i}^\sigma b b_{i,n}^\sigma & \cdots & a_{n,n}^\sigma b^{-1}b_{n,n-1}^\sigma + \sum_{i<n} b^{-1}a_{n,i}^\sigma b_{i,n-1}^\sigma \\ ba_{1,n}^\sigma b_{n,n}^\sigma + \sum_{i<n} a_{1,i}^\sigma b b_{i,n}^\sigma & \cdots & ba_{1,n}^\sigma b^{-1}b_{n,n-1}^\sigma + \sum_{i<n} a_{1,i}^\sigma b_{i,n-1}^\sigma \\ \vdots & \ddots & \vdots \\ ba_{n-1,n}^\sigma b_{n,n}^\sigma + \sum_{i<n} a_{n-1,i}^\sigma b b_{i,n}^\sigma & \cdots & ba_{n-1,n}^\sigma b^{-1}b_{n-1,n-1}^\sigma + \sum_{i<n} a_{n-1,i}^\sigma b_{i,n-1}^\sigma \end{bmatrix}. \end{aligned}$$

An observation says these two computations agree.

Next to check $GL_n(K)^{\mu_n} = A^\times$. The backward inclusion follows by the following computation:

$$\sigma \cdot \begin{bmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ ba_n^\sigma & a_1^\sigma & \cdots & a_{n-2}^\sigma & a_{n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ba_2^{\sigma^{n-1}} & ba_3^{\sigma^{n-1}} & \cdots & ba_n^{\sigma^{n-1}} & a_1^{\sigma^{n-1}} \end{bmatrix} = \begin{bmatrix} a_1^{\sigma^{n-1}\sigma} & b^{-1}ba_2^{\sigma^{n-1}\sigma} & \cdots & b^{-1}ba_{n-2}^{\sigma^{n-1}\sigma} & b^{-1}ba_2^{\sigma^{n-1}\sigma} \\ ba_n^\sigma & a_1^\sigma & \cdots & a_{n-2}^\sigma & a_{n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ba_2^{\sigma^{n-2}\sigma} & ba_3^{\sigma^{n-2}\sigma} & \cdots & ba_n^{\sigma^{n-2}\sigma} & a_1^{\sigma^{n-2}\sigma} \end{bmatrix}$$

$$= \begin{bmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ ba_n^\sigma & a_1^\sigma & \cdots & a_{n-2}^\sigma & a_{n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ ba_2^{\sigma^{n-1}} & ba_3^{\sigma^{n-1}} & \cdots & ba_n^{\sigma^{n-1}} & a_1^{\sigma^{n-1}} \end{bmatrix}.$$

For the forward inclusion, suppose $(a_{ij}) \in GL_n(K)^{\mu_n}$. If $\sigma \cdot (a_{i,j}) = (a_{i,j})$, then $\sigma^k \cdot (a_{i,j}) = (a_{i,j})$. Hence it suffices to look at

$$\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \begin{bmatrix} a_{nn}^\sigma & b^{-1}a_{n,1}^\sigma & \cdots & b^{-1}a_{n,n-1}^\sigma \\ ba_{1,n}^\sigma & a_{1,1}^\sigma & \cdots & a_{1,n-1}^\sigma \\ \vdots & \vdots & \ddots & \vdots \\ ba_{n-1,n}^\sigma & a_{n-1,1}^\sigma & \cdots & a_{n-1,n-1}^\sigma \end{bmatrix}.$$

The diagonal entries give $a_{1,1} = a_{n,n}^\sigma = a_{n-1,n-1}^{\sigma^2} = \cdots = a_{2,2}^{\sigma^{n-1}}$, so the diagonal is of the form satisfied by elements of $A^\times$. Now look at the (i,j) entry for $i < j$. We have

$$a_{i,j} = \begin{cases} b^{-1}a_{n,j-1}^\sigma & \text{if } i = 1, \\ a_{i-1,j-1}^\sigma & \text{if } i > 1. \end{cases}$$

Similarly, looking at the (i,j) entry for $i > j$, we have

$$a_{i,j} = \begin{cases} ba_{i-1,n}^\sigma & \text{if } j = 1, \\ a_{i-1,j-1}^\sigma & \text{if } i > 1. \end{cases}$$

This says the other diagonals are also of the form corresponding to an element of $A^\times$, so $(a_{i,j}) \in A^\times$.

Finally, for the last part, we know by proposition 2.1 that every element in W can be represented by a corresponding permutation matrix of S_n. Hence the action of σ on W corresponds to the diagonal shifting action on S_n, which we know is conjugation by $(1\ 2\ \cdots\ n)$. □

Following the discussion at the end of the introduction, we now give an application of theorem 1.1.

Corollary 2.3. *Suppose K has characteristic zero. Let K^{sep} be a separable closure of K such that its absolute Galois group $\Gamma = \mathrm{Gal}(K^{sep}/K)$ has cardinality two. Then $H^1(\Gamma, N)$ has cardinality 2.*

Proof. Theorem 1.1 tells us it suffices to find two elements of $Z^1(\mu_2, N)$ that cannot be identified under the equivalence relation of $H^1(\mu_2, N)$. Consider $f, g \in Z^1(\mu_2, N)$ defined by

$$f(\sigma) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad g(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where $\sigma = (1\ 2) \in S_2$. They are distinct because K is not of characteristic two. If $f \sim g$, then there exists a matrix $\omega \in N$ with $f(\sigma) = \omega g(\sigma)(\sigma \cdot \omega^{-1})$. Note that

$$\omega = \begin{bmatrix} 0 & x \\ y & 0 \end{bmatrix} \qquad \text{or} \qquad \omega = \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$$

for some $x, y \in K^\times$. In the first case we would have

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = f(\sigma) = \omega g(\sigma)(\sigma \cdot \omega^{-1}) = \begin{bmatrix} 0 & -b^{-1} \\ -b & 0 \end{bmatrix},$$

giving a contradiction as this implies $1 = b = -1$. In the second case we would have

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = f(\sigma) = \omega g(\sigma)(\sigma \cdot \omega^{-1}) = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix},$$

again another contradiction. □

3. Proof of theorem 1.1

Let us write $G := \mu_n$ and preserve the notations in section 2. Since T is normal in N, it is known [7, chapter I, proposition 38] that the exact sequence $0 \longrightarrow T \longrightarrow N \xrightarrow{p} W \longrightarrow 0$ induces an exact sequence of pointed sets

$$H^1(G,T) \longrightarrow H^1(G,N) \xrightarrow{p_*} H^1(G,W),$$

where the first set is a group, the basepoints of the other two sets are the trivial maps $x \mapsto \mathrm{Id}_n$, and p_* is defined by $p_*(f) = pf$. We first show that:

Proposition 3.1. $H^1(G,T) = 0$.

Proof. A free resolution for $\mathbb{Z}[\mu_n] = \mathbb{Z}[t]/(t^n-1)$ is given by

$$\mathbb{Z} \xleftarrow{1\leftarrow t} \mathbb{Z}[t]/(t^n-1) \xleftarrow{t-1} \mathbb{Z}[t]/(t^n-1) \xleftarrow{t^{n-1}+t^{n-2}+\cdots+t+1} \mathbb{Z}[t]/(t^n-1) \xleftarrow{t-1} \mathbb{Z}[t]/(t^n-1) \longleftarrow \cdots$$

By applying $\mathrm{Hom}_{\mathbb{Z}[G]}(-,T)$, we get

$$T \xrightarrow{t-1} T \xrightarrow{t^{n-1}+t^{n-2}+\cdots+t+1} T \xrightarrow{t-1} T \longrightarrow \cdots .$$

Write each element of T as $(t_1,\ldots,t_n)$, where the column vector t_i has only nonzero entry at entry i. Abusing notation we will also say t_i is its nonzero entry. To show $H^1(G,T) = 0$, we need to show that

$$\begin{aligned}\{(t_n^\sigma t_1^{-1}, t_1^\sigma t_2^{-1}, \ldots, t_{n-1}^\sigma t_n^{-1})\} &\overset{?}{=} \{(t_1,\ldots,t_n) : (t_2^{\sigma^{n-1}} t_3^{\sigma^{n-2}} \cdots t_n^\sigma t_1, \ldots, t_1^{\sigma^{n-1}} t_2^{\sigma^{n-2}} \cdots t_{n-1}^\sigma t_n) = 1\} \\ &= \{(t_1,\ldots,t_n) : t_1^{-1} = t_2^{\sigma^{n-1}} t_3^{\sigma^{n-2}} \cdots t_n^\sigma\}.\end{aligned}$$

For the forward inclusion, we check that indeed

$$(t_1^\sigma t_2^{-1})^{\sigma^{n-1}} (t_2^\sigma t_3^{-1})^{\sigma^{n-2}} \cdots (t_{n-1}^\sigma t_n^{-1})^\sigma = t_1 t_n^{-\sigma} = (t_n^\sigma t_1^{-1})^{-1}.$$

For the reverse inclusion, suppose $(t_1,\ldots,t_n)$ has the property of the right hand side. We want to find $u_1,\ldots,u_n$ such that $(u_n^\sigma u_1^{-1}, u_1^\sigma u_2^{-1}, \ldots, u_{n-1}^\sigma u_n^{-1}) = (t_1,\ldots,t_n)$. Set $u_1 = 1$, and for $2 \le k \le n-1$ inductively set $u_k^{-1} u_{k-1}^\sigma = t_k$. This implies $u_n^\sigma = t_1$. It remains to see at the last coordinate the resulting u_n agrees with this. But

$$u_n^{-1} = u_{n-1}^{-\sigma} t_n = u_{n-2}^{\sigma^2} t_{n-1}^\sigma t_n = \cdots = t_2^{\sigma^{n-2}} t_3^{\sigma^{n-3}} \cdots t_{n-1}^\sigma t_n = t_1^{-\sigma^{n-1}},$$

so $u_n^\sigma = t_1$ as desired. In fact, this proof tells us $H^k(G,T) = 0$ for all odd positive integers k, but this does not help much as our exact sequence ends at the first cohomology. □

Note that $H^1(G,T) = 0$ does not imply p_* is injective in general, but in our case it does. Let us first grant ourself this result. Then it remains to show that $H^1(G,W)$ has cardinality the claimed value p_n. Notice every function f in $H^1(G,W)$ can be specified by just knowing $f(\sigma)$. This is because the condition of f implies

$$\begin{aligned}f(\sigma^k) &= f(\sigma)(\sigma \cdot f(\sigma^{k-1})) \\ &= f(\sigma)(\sigma \cdot f(\sigma))(\sigma^2 \cdot f(\sigma^{k-2})) \\ &= \cdots \\ &= f(\sigma)(\sigma \cdot f(\sigma))(\sigma^2 \cdot f(\sigma)) \cdots (\sigma^{k-1} \cdot f(\sigma)) \\ &= (f(\sigma)\sigma)^k \sigma^{-k}.\end{aligned}$$

In particular $1 = (f(\sigma)\sigma)^n$ since $f(1) = f(1)(1 \cdot f(1)) = f(1)^2$ implies $f(1) = 1$. Hence we can associate each $f \in Z^1(G,W)$ with the value $f(\sigma)$. Let S be the set of n-torsion elements in S_n, and P be the set S modulo conjugation. We need to show P is in bijection with $H^1(G,W)$. Define a map

$$S \longrightarrow Z^1(G,W) \qquad \text{by} \qquad k \mapsto k\sigma^{-1}.$$

This map is clearly injective. For surjectivity, if $\tau \in Z^1(G,W)$ then by assumption $(\tau\sigma)^n = 1$, hence $\tau\sigma \in S$ maps to τ. Notice the map above also preserves relations, since if $k' \sim \omega k \omega^{-1}$ in P, then $k'\sigma^{-1} \sim \omega k \omega^{-1}\sigma^{-1} = \omega k \sigma^{-1} \sigma \omega^{-1} \sigma^{-1} = \omega k \sigma^{-1}(g \cdot \omega^{-1})$ in $H^1(G,W)$. Therefore this descends to a bijective map

from P to $H^1(G,W)$, and $H^1(G,W)$ has cardinality as claimed since it is well-known S has cardinality precisely p_n (as defined in theorem 1.1).

It remains to show p_* is injective. To do this, we need to introduce twisting. For a cohomology group $H^1(G,K)$ and an element $k \in Z^1(G,K)$, its k^{th}-*twist* $H^1(G,K)_k$ is defined by giving a new action of G on K as $\tau \cdot_k k' = k(\tau)(\tau \cdot k')k(\tau)^{-1}$. By noticing that T normalizes N, the same arguments as in [7, chapter I, section 5.3] tells us:

Proposition 3.2. *For each $k \in H^1(G,N)$, the map between $H^1(G,T)_k$ and $H^1(G,T)$ defined by $k' \mapsto kk'$ is a bijection that respects the G-action.* □

We are finally able to complete our proof of theorem 1.1.

Proposition 3.3. *$H^1(G,N)$ injects into $H^1(G,W)$.*

Proof. As T is a subgroup of N, we get a natural multiplication map $m : T \times N \longrightarrow N$. However we know from proposition 2.2 that there is a G-action on T and N, so m is also a G-map. This induces a map on cohomology groups

$$H^1(G,T) \times H^1(G,N) \xrightarrow{i} H^1(G, T \times N) \xrightarrow{m_*} H^1(G,N),$$

where the first map is defined by $i(f,g)(\tau) = (f(\tau), g(\tau))$. Notice i is a bijection, so in fact we still get an action of $H^1(G,T)$ on $H^1(G,N)$ simply by pointwise multiplication. This action restricts to $p_*^{-1}(w)$ for any $w \in H^1(G,W)$. To see this, suppose $l \in p^{-1}(w)$ and $u \in H^1(G,T)$. Then for any $\tau \in G$,

$$p_*(u(\tau)l(\tau)) = p_*(l(\tau)u'(\tau)) = w(\tau)p_*(u(\tau)) = w(\tau) = p_*(l(\tau)),$$

where $u'(\tau)$ is defined by $l(\tau)^{-1}u(\tau)l(\tau)$ (notice this still lies in T as $l(\tau)$ lies in the normalizer N of T by definition).

Now suppose $p_*(f) = p_*(g)$. Then there exists $\omega \in W$ with $pg(\tau) = \omega(pf(\tau))(\tau \cdot \omega^{-1})$ for all $\tau \in G$. This implies in $Z^1(G,N)$ that

$$g(\tau)t'(\tau) = \omega f(\tau)(\tau \cdot \omega^{-1})$$

for some function $t' : G \longrightarrow T$. By a similar argument as above we can find a function $t : G \longrightarrow T$ such that $tg = gt'$. Now for $\tau_1, \tau_2 \in G$ a calculation tells us

$$\begin{aligned} t(\tau_1\tau_2)g(\tau_1\tau_2) &= \omega f(\tau_1\tau_2)(\tau_1\tau_2 \cdot \omega^{-1}) \\ &= \omega f(\tau_1)(\tau_1 \cdot f(\tau_2))(\tau_1\tau_2 \cdot \omega^{-1}) \\ &= \omega f(\tau_1)(\tau_1 \cdot \omega^{-1})(\tau_1 \cdot (\omega f(\tau_2)(\tau_2 \cdot \omega^{-1}))) \\ &= t(\tau_1)g(\tau_1)(\tau_1 \cdot t(\tau_2))(\tau_1 \cdot g(\tau_2)), \end{aligned}$$

so tg is also a cocycle in $H^1(G,N)$. However this also tells us that

$$t(\tau_1\tau_2) = t(\tau_1)g(\tau_1)(\tau_1 \cdot t(\tau_2))g(\tau_1)^{-1},$$

so t is not in $H^1(G,T)$. However we see that t lives in $H^1(G,T)_g$. By proposition 3.2 we get an action

$$H^1(G,N) \times H^1(G,T)_g \xrightarrow{\mathrm{Id} \times \alpha_g} H^1(G,N) \times H^1(G,T) \xrightarrow{i} H^1(G, T \times N) \xrightarrow{m_*} H^1(G,N).$$

This tells us by fixing g and varying f that $H^1(G,T)_g$ acts transitively on $H^1(G,N)$. But $H^1(G,T)$ is trivial by proposition 3.1, so in fact $f = g$ in $H^1(G,N)$. □

4. An example of a cyclic division algebra

Let A be a cyclic algebra. In this section we will show that, under more assumptions on K and L, we can always choose $b \in L^\times$ such that A is a division algebra. Recall the (reduced) norm $\mathrm{Nm}(\alpha)$ of $\alpha \in A$ is defined to be the determinant of the matrix of α under right multiplication. Also recall Wedderburn's criterion [9], which says that A is a division algebra if and only if $\min\{l \in \mathbb{Z}_{>0} : b^l \in \mathrm{Nm}(K^\times)\} = n$. We use this to show the existence of such a b.

Proposition 4.1. *Let K and L be local fields. Then there exists some $b \in L^\times$ such that A is a cyclic division algebra. In fact, the proportion of elements in $L^\times$ that can be chosen as a candidate of b to make A a cyclic division algebra is $\phi(n)/n$, where ϕ is Euler's totient function.*

Proof. Since $\mathrm{Gal}(K/L)$ is cyclic of order n, hence abelian, by the local reciprocity law $L^\times/\mathrm{Nm}(K^\times) \cong \mathbb{Z}/n\mathbb{Z}$. Therefore $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ corresponds to some $b\,\mathrm{Nm}(K^\times) \neq \mathrm{Nm}(K^\times)$, i.e. that $b \notin \mathrm{Nm}(K^\times)$. It follows that $b, \dots, b^{n-1} \notin \mathrm{Nm}(K^\times)$, and we conclude by Wedderburn's criterion. The final claim follows trivially. □

Example of $\mathbb{Q}_l[\mu_{p^k}]$. Let us now give a computational example of finding such an element b. For distinct primes p and l, write $\mathbb{Q}_l$ to be the field of l-adic numbers, and write μ_{p^α} to be the set of p^α-roots of unity. We now try to search for some b that makes A a division algebra in the case $K = \mathbb{Q}_l[\mu_{p^k}]$ and $L = K^{\mu_n}$ with $n \neq 1$ dividing $l-1$ (the case $n = 1$ is highly uninteresting, since $A \cong K$ is certainly a division algebra over $L = K$). Note that the extension K/L is Galois and $\mathrm{Gal}(K/L) = \mu_n$. It is also a well-known fact that $\mu(\mathbb{Q}_l) = \mu_{l-1}$ is contained in L. Since $\mu_n \leq \mu_{l-1}$, the action of σ on $\mathbb{Q}_l$ is trivial, and $\sigma \cdot \zeta = \zeta^\sigma$ for each $\zeta \in \mu_{p^k}$. Observe the following easy fact.

Lemma 4.2. *Suppose $l - 1 = nm$ with $\gcd(n, m) = g$, and let d be a positive divisor of n^2. If gn^2/d divides $l - 1$, then $d \geq n$.*

Proof. Write $l - 1 = xyg^2$, where $x = n/g$ and $y = m/g$ are coprime. If $gn^2/d = g^3x^2/d$ divides $l - 1$, then we certainly need $g^3x^2/d \leq xyg^2$, so that $d \geq xg/y = nm/g \geq n$. □

Using this, we can show b can be chosen to be something simple.

Proposition 4.3. *If $l - 1 = nm$ with $\gcd(n, m) = g$ and b is a primitive root of μ_{gn}, then A is a division algebra containing all $(gn)^{th}$ roots of unity. In particular, for the case $\mathrm{Gal}(K/L) = \mu_{l-1}$, letting b be a primitive root of μ_{l-1} makes A into a division algebra.*

Proof. Suppose Wedderburn's criterion does not hold. Then $b^w \in \mathrm{Nm}(K^\times)$ for some $w \in \{1, \dots, n-1\}$. Say $b^w = \mathrm{Nm}(k)$ for some $k = \sum_{j=0}^{p^k-1} k_j\zeta^j \in K$, where $\langle\zeta\rangle = \mu_{p^k}$ and each $k_j \in \mathbb{Q}_l$. Then

$$b^w = \prod_{\sigma\in\mu_n} \sigma(k) = \prod_{\sigma\in\mu_n} \sum_{j=0}^{p^k-1} k_j\zeta^{j\sigma} = \sum_{j_1,\dots,j_n\in\{0,\dots,p^k-1\}} k_{j_1}\cdots k_{j_n}\zeta^{(j_1+\cdots+j_n)\sigma}.$$

Now, by comparing coefficients and summing them up,

$$b^w = \sum_{j_1,\dots,j_n\in\{0,\dots,p^k-1\}} k_{j_1}\cdots k_{j_n} = \left(\sum_{j=0}^{p^k-1} k_j\right)^n.$$

Write $\mathcal{K} = \sum_{j=0}^{p^k-1} k_j$ and $\gcd(w, n) = d$. Then b^w has order gn/d, so $\mathcal{K}$ is a primitive $(gn^2/d)^{th}$ root of unity. Lemma 4.2 then implies that $n = d$, so that $w \geq n$, a contradiction to our choice of w. □

We can say something more if we choose n such that n is coprime with $(l-1)/n$.

Proposition 4.4. *If $l-1 = nm$ and b is a primitive root of $\mu_{gn} \leq \mu_{l-1}$ that makes A into a division algebra, then $\gcd(n, m) \neq rg$ for any $r > 1$.*

Proof. Suppose $\gcd(n, m) = rg$. Then pick $w = \frac{n}{rg} < n$, so that b^w is a primitive $(rg)^{th}$ root of unity. Certainly $\gcd(w, n) = \frac{n}{rg}$, so $\frac{n^2}{w} = rgn$ divides $l - 1$. Therefore $\mathbb{Q}_l$, and hence $\mathbb{Q}_l[\mu_{p^k}]$, contains μ_{rgn}. Pick the $(rgn)^{th}$ root of unity ω where $\omega^n = b^w$. Then $\mathrm{Nm}(\omega) = b^w$, so that A is not a division algebra by Wedderburn's criterion, a contradiction. □

Corollary 4.5. *Let b be a primitive root of $\mu_n \leq \mu_{l-1}$ and $l - 1 = nm$. Then n and m are coprime if and only if A is a division algebra.*

Proof. This is a combination of the results from the previous two propositions. □

Let us now write $\mu_{p^\infty} = \bigcup_{\alpha\in\mathbb{Z}_{>0}} \mu_{p^\alpha}$, which is a countable set.

Corollary 4.6. *Propositions 4.3 and 4.4 holds in the case $K = \mathbb{Q}_l[\mu_{p^\infty}]$.* □

Proof. As every element in $\mathbb{Q}_l[\mu_{p^\infty}]$ is a finite linear combination in μ_{p^∞} with coefficients in $\mathbb{Q}_l$, it is contained in some $\mathbb{Q}_l[\mu_{p^k}]$ for sufficiently large k. □

Acknowledgements

This research project was performed under the mentorship of Craig Westerland, with support from the University of Minnesota's Undergraduate Research Opportunities Program.

References

[1] Saieed Akbari, Roohollah Ebrahimian, Momenaee Kermani, and Alireza Salehi Golsefidy, Maximal subgroups of $\mathrm{GL}_n(D)$, *J. Algebra* **259** (2003), 201–225.

[2] Douglas Bowman, Paul Erdos and Andrew M. Odlyzko, Partitions of n into parts which are divisors of n, *Amer. Math. Monthly* **99** (1992), 276–277.

[3] Helmut Hasse, Theory of cyclic algebras over an algebraic number field, *Trans. Amer. Math. Soc.* **34** (1932), 171–214.

[4] Roozbeh Hazrat and Adrian Wadsworth, On maximal subgroups of the multiplicative group of a division algebra, *J. Algebra* **322** (2009), 2528–2543.

[5] Jürgen Neukirch, *Algebraic number theory*, Springer-Verlag, 1999.

[6] Louis Rowen, *Graduate Algebra: Noncommutative View*, American Mathematical Society, 2008.

[7] Jean-Pierre Serre, *Galois Cohomology*, Springer, 1997.

[8] Uroyoán Walker, *On k-conjugacy classes of maximal tori in semi-simple algebraic groups*, Ph.D. thesis, Lousiana State University, 2001.

[9] Joseph Wedderburn, On division algebras, *Trans. Amer. Math. Soc.* **22** (1921), 129–135.